



DEFENSE INFORMATION SYSTEMS AGENCY

P. O. BOX 549
FORT MEADE, MARYLAND 20755-0549

IN REPLY
REFER TO: Joint Interoperability Test Command (JTE)

31 Oct 12

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Special Interoperability Test Certification of European Aeronautic Defense and Space Company (EADS) North America, Inc. Ectocryp Black Gateway with Software Release 1.1.3

References: (a) DoD Directive 4630.5, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)," 5 May 2004
(b) CJCSI 6212.01E, "Interoperability and Supportability of Information Technology and National Security Systems," 15 December 2008
(c) through (e), see Enclosure 1

1. References (a) and (b) establish the Defense Information Systems Agency (DISA), Joint Interoperability Test Command (JITC), as the responsible organization for interoperability test certification.

2. The EADS North America, Inc. Ectocryp Black Gateway with Software Release 1.1.3 is hereinafter referred to as the System Under Test (SUT). The SUT meets all of its critical interoperability requirements and is certified for joint use within the Defense Information System Network (DISN) as a DoD (Department of Defense) Secure Communications Device (DSCD). The SUT is certified for Secure Communications Internet Protocol (SCIP) with a Digital Transmission Link Level 1 (T1) Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) National ISDN 2 (NI2) American National Standards Institute (ANSI) T1.619a. The SUT was tested and is certified on the low side with the Avaya CS2100 and Siemens Elektronisches Wählsystem Digital (EWSD). JITC analysis determined that the SUT is also certified for joint use with any legacy Multifunction Switch, Small End Office, or Private Branch Exchange, and any Unified Capabilities (UC) Local Session Controller, Multifunction Soft Switch, or Wide Area Network (WAN) Soft Switch listed on the UC Approved Product List (APL) certified with the T1 ISDN PRI NI2 ANSI T1.619a interface. Furthermore, the SUT is certified on the high side T1 ISDN PRI NI2 ANSI T1.619a interface approved for use in a single security level secure network. The SUT must be deployed in accordance with References (c) and (d). The SUT meets the critical interoperability requirements set forth in Reference (e), using test procedures derived from Reference (f). No other configurations, features, or functions, except those cited within this report, are certified by the JITC. This certification expires upon changes that could affect interoperability, but no later than three years from the date of the Unified Capabilities (UC) Approved Products List (APL) memorandum.

3. This finding is based on interoperability testing, DISA adjudication of open test discrepancy reports (TDRs), review of the vendor's Letters of Compliance (LoC), and DISA Information

JITC Memo, JTE, Special Interoperability Test Certification of European Aeronautic Defense and Space Company (EADS) North America, Inc. Ectocryp Black Gateway with Software Release 1.1.3

Assurance Certifying Authority (CA) Recommendation for placement on the DoD UC APL. Interoperability testing was conducted by JITC at the GIG (Global Information Grid) Network Test Facility (GNTF), Fort Huachuca, Arizona, from 5 through 16 September 2011. Verification and Validation (V&V) testing was conducted by JITC at the GNTF, Fort Huachuca, Arizona, from 21 through 24 May 2012. Review of the vendors LoC was completed on 5 October 2011. DISA adjudication of open TDRs was completed on 20 December 2011. The DISA CA provided a positive recommendation on 31 October 2012 based on the security testing completed by DISA-led IA test Teams and published in a separate report, Reference (g). Enclosure 2 documents the test results and describes the test network and system configurations.

4. Table 1 provides the interoperability test summary of the SUT. Table 2 provides the UC DSCD Interoperability Requirements. The interoperability test status is based on the SUT's ability to meet:

- a. DISN services for Network and Applications specified in reference (e).
- b. DSCD interface and signaling requirements as specified in reference (e) verified through JITC testing and/or vendor submission of LoC.
- c. DSCD Capability Requirements (CRs)/Feature Requirements (FRs) specified in reference (e) verified through JITC testing and/or vendor submission of LoC.
- d. The overall system interoperability performance derived from test procedures listed in reference (f).

Table 1. SUT Interoperability Test Summary

DSCD Interoperability Requirements																							
Interface & Signaling	Critical	Status	Remarks																				
T1 ISDN PRI NI 1/2 (ANSI T1.619a)	Yes	Certified	Met all critical CRs and FRs with the following minor exceptions: The SUT does not support ISDN B Channel Availability (Service Messages). ¹ The SUT does not have an NSA Type 1 certification. ²																				
Security	Yes	Certified	Met all critical CRs and FRs. ³																				
<p>NOTES:</p> <p>1. The SUT does not support ISDN B Channel Availability (Service Messages). The SUT does not acknowledge or have the ability to initiate in-service or out-of-service Service Messages. To mitigate the impact of this discrepancy, the respective B channels must be busied out by both switches at each end of the circuit. DISA adjudicated this as having a minor operational impact based on the stipulation that this condition be noted in the SUT deployment guide. The vendor has no plans to fix this anomaly based on the following: The SUT is typically deployed in a local location resulting in short runs between the device and the high side and low side switches. This has resulted in there not being a customer requirement to automatically set the availability of channels.</p> <p>2. Since the SUT is a product of a foreign manufacturer, the SUT will not receive a NSA Type 1 certification; however, in lieu of NSA Type 1 certification, the SUT received an NSA Authority To Operate on 20 January 2012, which meets this requirement.</p> <p>3. Security is tested by DISA-led Information Assurance test teams and published in a separate report, Reference (e).</p> <p>LEGEND:</p> <table> <tr> <td>ANSI</td> <td>American National Standard Institute</td> <td>ISDN</td> <td>Integrated Services Digital Network</td> </tr> <tr> <td>CR</td> <td>Capability Requirements</td> <td>NI 1/2</td> <td>National ISDN standard 1 or 2</td> </tr> <tr> <td>DRSN</td> <td>Defense Red Switch Network</td> <td>PRI</td> <td>Primary Rate Interface</td> </tr> <tr> <td>DSCD</td> <td>DoD Secure Communications Devices</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>FR</td> <td>Functional Requirements</td> <td></td> <td></td> </tr> </table>				ANSI	American National Standard Institute	ISDN	Integrated Services Digital Network	CR	Capability Requirements	NI 1/2	National ISDN standard 1 or 2	DRSN	Defense Red Switch Network	PRI	Primary Rate Interface	DSCD	DoD Secure Communications Devices	SUT	System Under Test	FR	Functional Requirements		
ANSI	American National Standard Institute	ISDN	Integrated Services Digital Network																				
CR	Capability Requirements	NI 1/2	National ISDN standard 1 or 2																				
DRSN	Defense Red Switch Network	PRI	Primary Rate Interface																				
DSCD	DoD Secure Communications Devices	SUT	System Under Test																				
FR	Functional Requirements																						

Table 2. DSCD UCR Interoperability Requirements

DISN Trunk Interfaces																																															
Interface	Critical	Requirements Required or Conditional	References																																												
T1 ISDN PRI NI2 (ANSI T1.619a)	Yes	<ul style="list-style-type: none"> Type Approved by NSA. (R) The DSCD devices that use a 2-wire analog or BRI interface shall meet the EI requirements as specified in Section 5.2.1, Customer Premises Equipment Requirements. DSCD devices that support DISN trunk interfaces (PRI or IP [AS-SIP]) shall meet the interface requirements defined in 5.3.2.12.10, MG Support for ISDN. DSCD devices that support one of the required signaling modes shall go secure with 85% call completion rate. (R) Shall establish secure call within 60 seconds for duration of secure call. (R) Shall operate in a network that has an end-to-end latency of up to 600 milliseconds. (R) The DSCD shall achieve and maintain a secure voice connection with a minimum MOS of 3.0. (R) Shall obtain a new key and properly process the new key with a 95 percent completion rate. (R) 	UCR 2008, Change 3, Paragraph 5.2.2.2																																												
Security	Yes	<ul style="list-style-type: none"> GR-815, STIGs, and DoDI 8510.bb (DIACAP) (R) 	UCR 2008, Change 3, Section 5.4																																												
LEGEND: <table border="0"> <tr> <td>ANSI</td> <td>American National Standards Institute</td> <td>IP</td> <td>Internet Protocol</td> </tr> <tr> <td>AS-SIP</td> <td>Assured Services Session Initiation Protocol</td> <td>ISDN</td> <td>Integrated Services Digital Network</td> </tr> <tr> <td>BRI</td> <td>Basic Rate Interface</td> <td>MG</td> <td>Media Gateway</td> </tr> <tr> <td>DIACAP</td> <td>DoD Information Assurance Certification and Accreditation Process</td> <td>MOS</td> <td>Mean Opinion Score</td> </tr> <tr> <td>DoD</td> <td>Department of Defense</td> <td>NSA</td> <td>National Security Agency</td> </tr> <tr> <td>DoDI</td> <td>Department of Defense Instruction</td> <td>PRI</td> <td>Primary Rate Interface</td> </tr> <tr> <td>DSCD</td> <td>DoD Secure Communications Device</td> <td>R</td> <td>Required</td> </tr> <tr> <td>DISN</td> <td>Defense Information System Network</td> <td>STIGs</td> <td>Security Technical Implementation Guides</td> </tr> <tr> <td>EI</td> <td>End Instrument</td> <td>T1</td> <td>Digital Transmission Link Level 1 (1.544 Mbps)</td> </tr> <tr> <td>GR</td> <td>Generic Requirement</td> <td>T1.619a</td> <td>SS7 and ISDN MLPP Signaling Standard for T1</td> </tr> <tr> <td>GR-815</td> <td>Generic Requirements For Network Element/Network System (NE/NS) Security</td> <td>UCR</td> <td>Unified Capabilities Requirements</td> </tr> </table>				ANSI	American National Standards Institute	IP	Internet Protocol	AS-SIP	Assured Services Session Initiation Protocol	ISDN	Integrated Services Digital Network	BRI	Basic Rate Interface	MG	Media Gateway	DIACAP	DoD Information Assurance Certification and Accreditation Process	MOS	Mean Opinion Score	DoD	Department of Defense	NSA	National Security Agency	DoDI	Department of Defense Instruction	PRI	Primary Rate Interface	DSCD	DoD Secure Communications Device	R	Required	DISN	Defense Information System Network	STIGs	Security Technical Implementation Guides	EI	End Instrument	T1	Digital Transmission Link Level 1 (1.544 Mbps)	GR	Generic Requirement	T1.619a	SS7 and ISDN MLPP Signaling Standard for T1	GR-815	Generic Requirements For Network Element/Network System (NE/NS) Security	UCR	Unified Capabilities Requirements
ANSI	American National Standards Institute	IP	Internet Protocol																																												
AS-SIP	Assured Services Session Initiation Protocol	ISDN	Integrated Services Digital Network																																												
BRI	Basic Rate Interface	MG	Media Gateway																																												
DIACAP	DoD Information Assurance Certification and Accreditation Process	MOS	Mean Opinion Score																																												
DoD	Department of Defense	NSA	National Security Agency																																												
DoDI	Department of Defense Instruction	PRI	Primary Rate Interface																																												
DSCD	DoD Secure Communications Device	R	Required																																												
DISN	Defense Information System Network	STIGs	Security Technical Implementation Guides																																												
EI	End Instrument	T1	Digital Transmission Link Level 1 (1.544 Mbps)																																												
GR	Generic Requirement	T1.619a	SS7 and ISDN MLPP Signaling Standard for T1																																												
GR-815	Generic Requirements For Network Element/Network System (NE/NS) Security	UCR	Unified Capabilities Requirements																																												

5. No detailed test report was developed in accordance with the Program Manager’s request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssi>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil.

JITC Memo, JTE, Special Interoperability Test Certification of European Aeronautic Defense and Space Company (EADS) North America, Inc. Ectocryp Black Gateway with Software Release 1.1.3

6. The JITC point of contact is Ms. Anita Mananquil, DSN 879-5164, commercial (520) 538-5164, FAX DISN 879-4347, or e-mail to anita.l.mananquil.civ@mail.mil. The JITC's mailing address is P.O. Box 12798, Fort Huachuca, AZ 85670-2798. The tracking number for the SUT is 1108001.

FOR THE COMMANDER:



for RICHARD A. MEADOR
Chief
Battlespace Communications Portfolio

2 Enclosures a/s

Distribution (electronic mail):

DoD CIO

Joint Staff J-6, JCS

USD(AT&L)

ISG Secretariat, DISA, JTA

U.S. Strategic Command, J665

US Navy, OPNAV N2/N6FP12

US Army, DA-OSA, CIO/G-6 ASA(ALT), SAIS-IOQ

US Air Force, A3CNN/A6CNN

US Marine Corps, MARCORSYSCOM, SIAT, A&CE Division

US Coast Guard, CG-64

DISA/TEMC

DIA, Office of the Acquisition Executive

NSG Interoperability Assessment Team

DOT&E, Netcentric Systems and Naval Warfare

Medical Health Systems, JMIS IV&V

HQUSAISEC, AMSEL-IE-IS

UCCO

ADDITIONAL REFERENCES

- (c) National Security Agency “Memorandum for Approval to Operate the Ectocryp Black Gateway” dated 20 January 2012
- (d) Information Assurance Directorate “Operational Security Doctrine for the EADS Ectocryp Black Gateway DOC-021-11” dated November 2011
- (e) Office of the Assistant Secretary of Defense, “Department of Defense Unified Capabilities Requirements 2008, Change 3” September 2011
- (f) Joint Interoperability Test Command, “Defense Switched Network Generic Switch Test Plan (GSTP), Change 2,” 2 October 2006
- (g) Joint Interoperability Test Command, “Information Assurance (IA) Assessment of EADS Ectocryp Black with Release 1.1.3 (TN1108001),” 01 October 2012

CERTIFICATION TESTING SUMMARY

1. SYSTEM TITLE. European Aeronautic Defense and Space Company (EADS) North America, Inc. Ectocryp Black with Software Release 1.1.3; hereinafter referred to as the System Under Test (SUT).

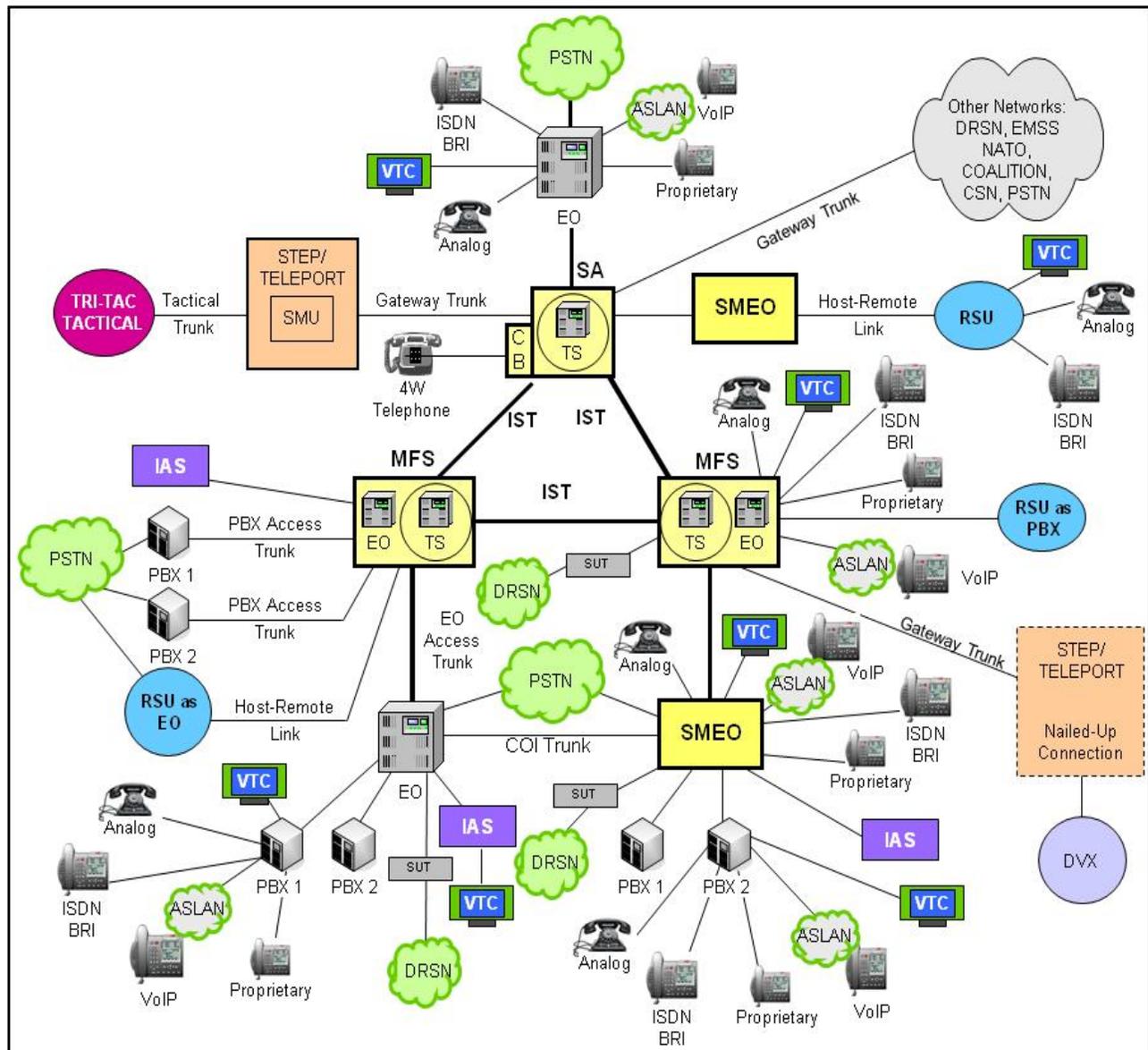
2. SPONSOR. Defense Information Systems Agency (DISA)

3. SYSTEM POC. Lou Schmuckler, GS24, Defense Information Systems Agency (DISA), 6916 Cooper Avenue, Fort Meade, MD, 20755, E-mail: Louis.a.schmuckler.civ@mail.mil.

4. TESTER. Joint Interoperability Test Command (JITC), Fort Huachuca, Arizona.

5. SYSTEM UNDER TEST DESCRIPTION. The SUT is a secure voice gateway that provides the capability for callers on a classified (Red) voice system to communicate with callers on an unclassified (low side) voice system, and vice versa. It achieves this by providing point-to-point Secure Communications Interoperability Protocol (SCIP) encryption for the duration of the telephone call, along with the added security of mutual authentication of the two callers. The call setup process is achieved through the SUT and DoD Secure Communication Devices (DSCDs) implementing SCIP. The SUT is certified for SCIP with a Digital Transmission Link Level 1 (T1) Integrated Services Digital Network (ISDN) Primary Rate Interface (PRI) National ISDN 2 (NI2) American National Standards (ANSI) Institute T1.619a. The SUT was tested and is certified on the low side with the Avaya CS2100 and Siemens Elektronisches Wählsystem Digital (EWSD). JITC analysis determined that the SUT is also certified for joint use with any legacy Multifunction Switch (MFS), Small End Office (SMEO), or Private Branch Exchange (PBX), and any Unified Capabilities (UC) Local Session Controller (LSC), Multifunction Soft Switch (MFSS), or Wide Area Network (WAN) Soft Switch (SS) listed on the UC Approved Product List (APL) certified with the T1 ISDN PRI NI2 ANSI T1.619a interface. Furthermore, the SUT is certified on the high side T1 ISDN PRI NI2 ANSI T1.619a interface approved for use in a single security level secure network. The SUT must be deployed in accordance with References (c) and (d).

6. OPERATIONAL ARCHITECTURE. The Defense Information System Network (DISN) architecture is a two-level network hierarchy consisting of DISN backbone switches and Service/Agency installation switches. Joint Staff policy and subscriber mission requirements determine which type of switch can be used at a particular location. The DISN architecture, therefore, consists of several categories of switches, including Private Branch Exchanges (PBX)s. The Unified Capabilities Requirements (UCR) operational DISN Architecture is depicted in Figure 2-1.



LEGEND:

ASLAN	Assured Services Local Area Network	NATO	North Atlantic Treaty Organization
4W	4-Wire	PBX	Private Branch Exchange
BRI	Basic Rate Interface	PBX 1	Private Branch Exchange 1
CB	Channel Bank	PBX 2	Private Branch Exchange 3
COI	Community of Interest	PSTN	Public Switched Telephone Network
CSN	Canadian Switch Network	RSU	Remote Switching Unit
DISN	Defense Information System Network	SMEO	Small End Office
DRSN	Defense Red Switch Network	SMU	Switched Multiplex Unit
DVX	Deployable Voice Exchange	STEP	Standardized Tactical Entry Point
EMSS	Enhanced Mobile Satellite System	SUT	System Under Test
EO	End Office	TDM/P	Time Division Multiplex/Packetized
IAS	Integrated Access Switch	Tri-Tac	Tri-Service Tactical Communications Program
ISDN	Integrated Services Digital Network	TS	Tandem Switch
IST	Interswitch Trunk	VoIP	Voice over Internet Protocol
MFS	Multifunction Switch	VTC	Video Teleconferencing

Figure 2-1. DISN Architecture

7. REQUIRED SYSTEM INTERFACES. The SUT Interoperability Test Summary is shown in Table 2-1 and the Capability and Feature Requirements used to evaluate the interoperability of the SUT are indicated in Table 2-2. These requirements are derived from the UCR and verified through JITC testing and review of the vendor's Letters of Compliance (LoC).

Table 2-1. SUT Interoperability Test Summary

DSCD Interoperability Requirements																							
Interface & Signaling	Critical	Status	Remarks																				
T1 ISDN PRI NI 1/2 (ANSI T1.619a)	Yes	Certified	Met all critical CRs and FRs with the following minor exceptions: The SUT does not support ISDN B Channel Availability (Service Messages). ¹ The SUT does not have an NSA Type 1 certification. ²																				
Security	Yes	Certified	Met all CRs and FRs ³																				
<p>NOTES:</p> <p>1. The SUT does not support ISDN B Channel Availability (Service Messages). The SUT does acknowledge or have the ability to initiate in-service or out-of-service Service Messages. To mitigate the impact of this discrepancy, the respective B channels must be busied out by both switches at each end of the circuit. DISA adjudicated this as having a minor operational impact based on the stipulation that this condition be noted in the SUT deployment guide. The vendor has no plans to fix this anomaly based on the following: The SUT is typically deployed in a local location resulting in short runs between the device and the high and low switches. This has resulted in there not being a customer requirement to automatically set the availability of channels.</p> <p>2. Since the SUT is a product of a foreign manufacturer, the SUT will not receive a NSA Type 1 certification; however, in lieu of NSA Type 1 certification the SUT received an Authority To Operate from NSA on January 20, 2012, which meets this requirement.</p> <p>3. Security is tested by DISA-led Information Assurance test teams and published in a separate report, Reference (e).</p> <p>LEGEND:</p> <table border="0"> <tr> <td>ANSI</td> <td>American National Standard Institute</td> <td>ISDN</td> <td>Integrated Services Digital Network</td> </tr> <tr> <td>CR</td> <td>Capability Requirements</td> <td>NI 1/2</td> <td>National ISDN standard 1 or 2</td> </tr> <tr> <td>DISA</td> <td>Defense Information Systems Agency</td> <td>PRI</td> <td>Primary Rate Interface</td> </tr> <tr> <td>DSCD</td> <td>DoD Secure Communications Devices</td> <td>SUT</td> <td>System Under Test</td> </tr> <tr> <td>FR</td> <td>Feature Requirements</td> <td></td> <td></td> </tr> </table>				ANSI	American National Standard Institute	ISDN	Integrated Services Digital Network	CR	Capability Requirements	NI 1/2	National ISDN standard 1 or 2	DISA	Defense Information Systems Agency	PRI	Primary Rate Interface	DSCD	DoD Secure Communications Devices	SUT	System Under Test	FR	Feature Requirements		
ANSI	American National Standard Institute	ISDN	Integrated Services Digital Network																				
CR	Capability Requirements	NI 1/2	National ISDN standard 1 or 2																				
DISA	Defense Information Systems Agency	PRI	Primary Rate Interface																				
DSCD	DoD Secure Communications Devices	SUT	System Under Test																				
FR	Feature Requirements																						

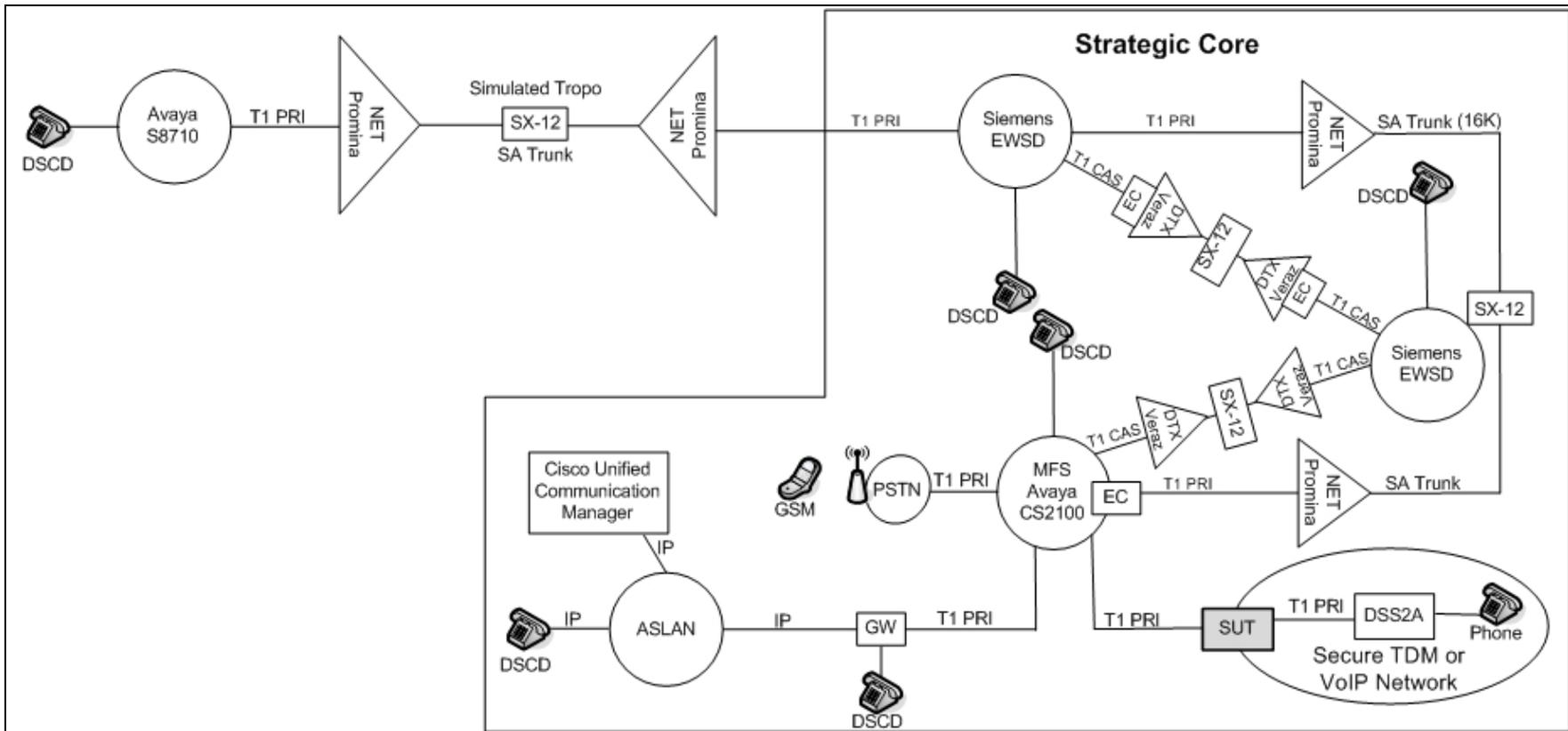
Table 2-2. DSCD UCR Interoperability Requirements

DISN Trunk Interfaces			
Interface	Critical	Requirements Required or Conditional	References
T1 ISDN PRI NI2 (ANSI T1.619a)	Yes	<ul style="list-style-type: none"> Type Approved by NSA. (R) The DSCD devices that use a 2-wire analog or BRI interface shall meet the EI requirements as specified in Section 5.2.1, Customer Premises Equipment Requirements. DSCD devices that support DISN trunk interfaces (PRI or IP [AS-SIP]) shall meet the interface requirements defined in 5.3.2.12.10, MG Support for ISDN. DSCD devices that support one of the required signaling modes shall go secure with 85% call completion rate. (R) Shall establish secure call within 60 seconds for duration of secure call. (R) Shall operate in a network that has an end-to-end latency of up to 600 milliseconds. (R) The DSCD shall achieve and maintain a secure voice connection with a minimum MOS of 3.0. (R) Shall obtain a new key and properly process the new key properly process the new key with a 95 percent completion rate. (R) 	UCR 2008, Change 3, Paragraph 5.2.2.2
Security	Yes	<ul style="list-style-type: none"> GR-815, STIGs, and DoDI 8510.bb (DIACAP) (R) 	UCR 2008, Change 3, Section 5.4

Table 2-2. DSCD UCR Interoperability Requirements (continued)

LEGEND:			
ANSI	American National Standards Institute	IP	Internet Protocol
AS-SIP	Assured Services Session Initiation Protocol	ISDN	Integrated Services Digital Network
BRI	Basic Rate Interface	kbps	kilobits per second
DIACAP	DoD Information Assurance Certification and Accreditation Process	MG	Media Gateway
DoD	Department of Defense	MOS	Mean Opinion Score
DoDI	Department of Defense Instruction	NSA	National Security Agency
DSCD	DoD Secure Communications Device	PRI	Primary Rate Interface
DISN	Defense Information System Network	R	Required
EI	End Instrument	STIGs	Security Technical Implementation Guides
GR	Generic Requirement	T1	Digital Transmission Link Level 1 (1.544 Mbps)
GR-815	Generic Requirements For Network Element/Network System (NE/NS) Security.	T1.619a	SS7 and ISDN MLPP Signaling Standard for T1
		UCR	Unified Capabilities Requirements

8. TEST NETWORK DESCRIPTION. The SUT was tested at JITC’s Global Information Grid Network Test Facility in a manner and configuration similar to that of the DISN operational environment. Testing of the SUT required functions and features was conducted using the test configurations depicted in Figures 2-2 through 2-7. Figures 2-2 through 2-7 simulate actual DoD operationally deployed network to strategic core network test configuration strings. The SUT was tested as a secure voice gateway that provided the capability for callers on a classified (Red) voice system to communicate with callers on an unclassified (low side) voice system, and vice versa with DSCD devices located at various tests points denoted in each figure.



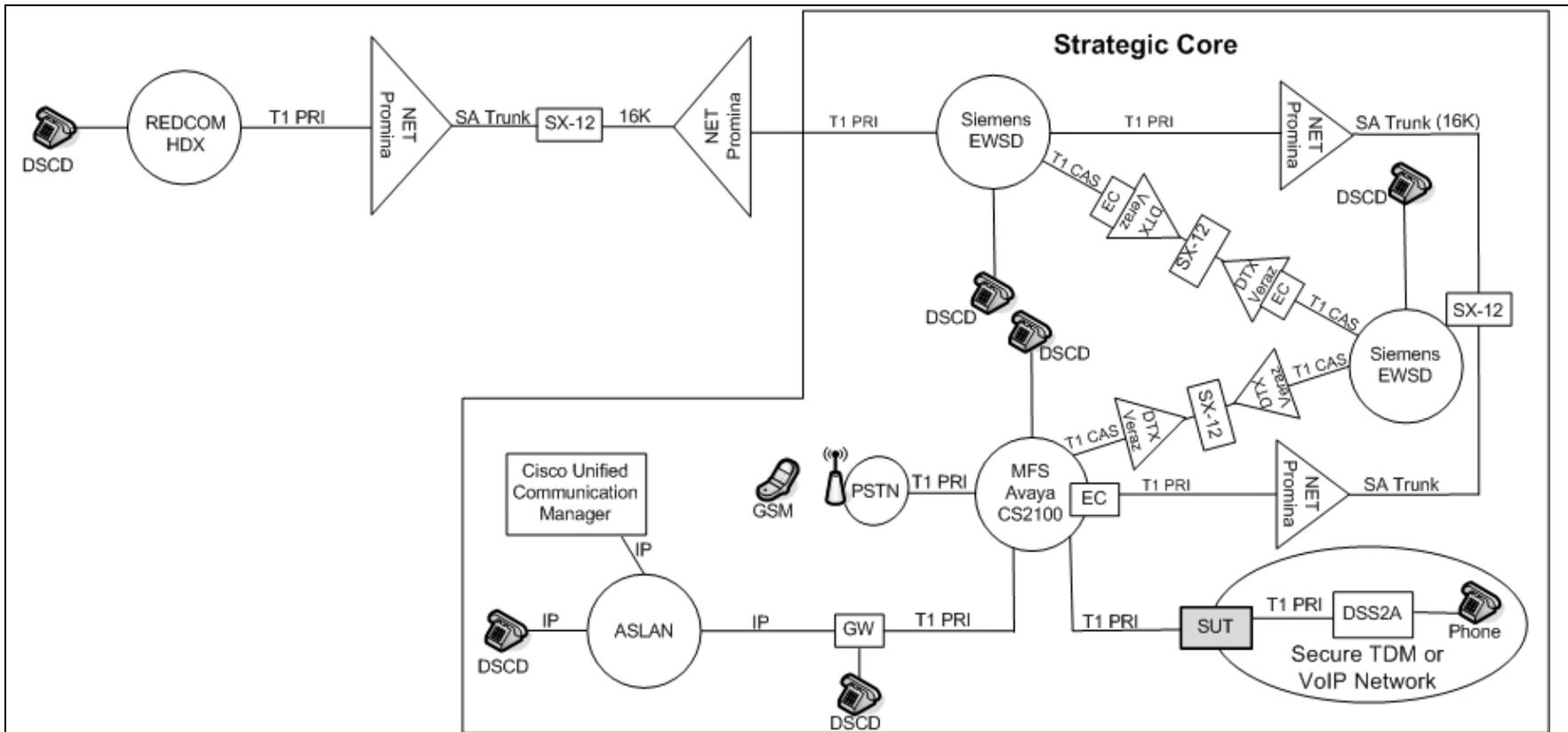
LEGEND:

ASLAN Assured Services Local Area Network
 CAS Channel Associated Signaling
 CEU Channel Encryption Unit
 CS2100 Communication Server 2100
 DSCD Department of Defense (DoD) Secure Communications Device
 EC Echo Cancellor
 EWSD Elektronisches Wählsystem Digital
 GSM Global System for Mobile Communications

GW Gateway
 IP Internet Protocol
 K Kilobit
 Mbps Megabits per second
 MFS Multifunction Switch
 NET Network Equipment Technology
 PRI Primary Rate Interface
 PSTN Public Switched Telephone Network
 SA Satellite Access

STE Secure Telephone Equipment
 SUT System Under Test
 SWT Sectéra® Wireline Terminal
 SX-12 Simulator, Data Link
 T1 Digital Transmission Link Level 1 (1.544 Mbps)
 TDM Time Division Multiplexing
 Tropo Tropospheric Scatter Radio
 VoIP Voice over Internet Protocol

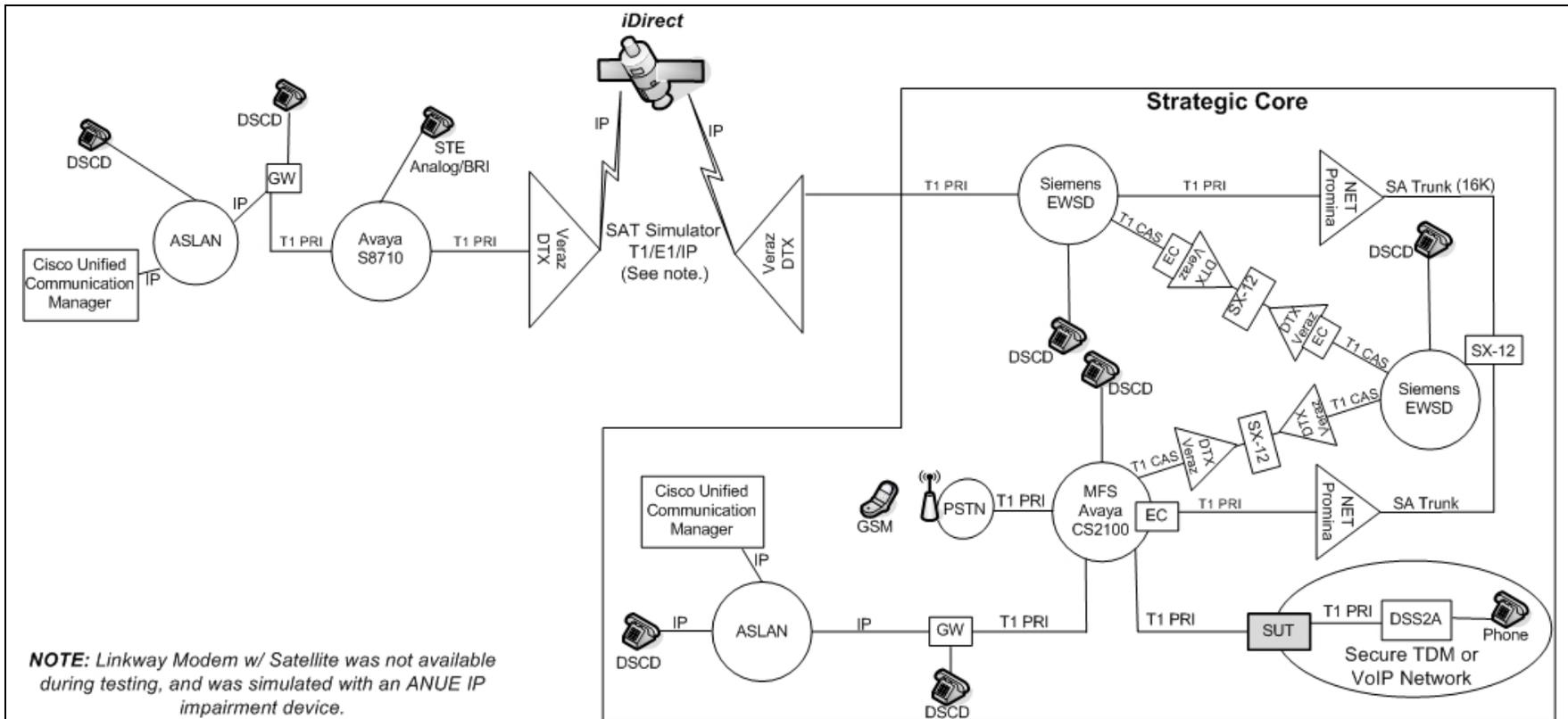
Figure 2-3. Air Force Composite Test Diagram



LEGEND:

ASLAN	Assured Services Local Area Network	GSM	Global System for Mobile Communications	SA	Satellite Access
CAS	Channel Associated Signaling	GW	Gateway	SAT	Subscriber Access Termination
CENTCOM	Central Command	IP	Internet Protocol	STE	Secure Telephone Equipment
CEU	Channel Encryption Unit	K	Kilobit	SUT	System Under Test
CS2100	Communication Server 2100	Mbps	Megabits per second	SWT	Sectéra® Wireline Terminal
DSCD	Department of Defense (DoD) Secure Communications Device	MFS	Multifunction Switch	SX-12	Simulator, Data Link
EC	Echo Canceller	NET	Network Equipment Technology	T1	Digital Transmission Link Level 1 (1.544 Mbps)
EWSD	Elektronisches Wählsystem Digital	PRI	Primary Rate Interface	TDM	Time Division Multiplexing
		PSTN	Public Switched Telephone Network	VoIP	Voice over Internet Protocol

Figure 2-4. CENTCOM Dual Hop Composite Test Diagram



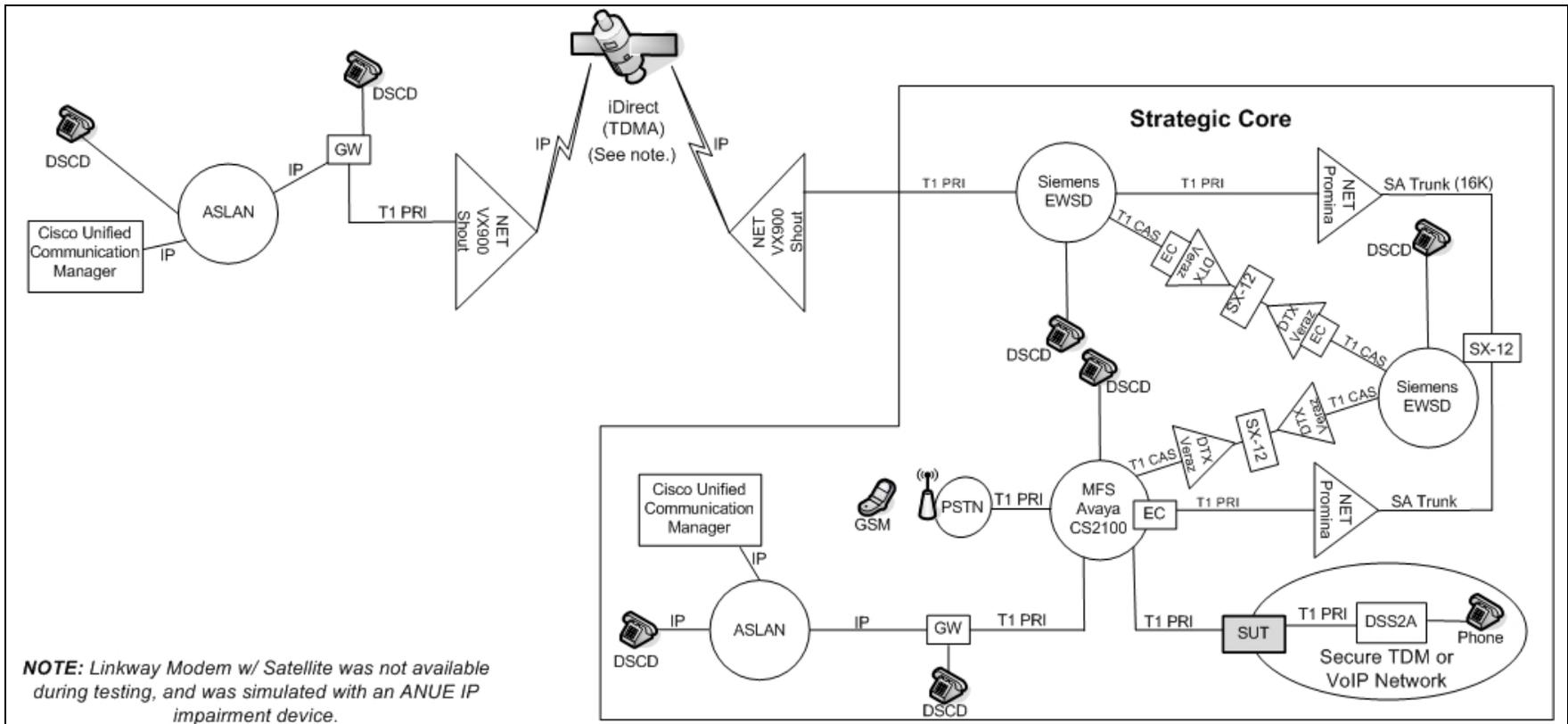
LEGEND:

ASLAN Assured Services Local Area Network
 CAS Channel Associated Signaling
 CENTCOM Central Command
 CEU Channel Encryption Unit
 CS2100 Communication Server 2100
 DSCD Department of Defense (DoD) Secure Communications Device
 E1 European Basic Multiplex Rate (2.048 Mbps)
 EC Echo Canceller

EWSD Elektronisches Wählsystem Digital
 GSM Global System for Mobile Communications
 GW Gateway
 IP Internet Protocol
 K Kilobit
 Mbps Megabits per second
 MFS Multifunction Switch
 NET Network Equipment Technology
 PRI Primary Rate Interface
 PSTN Public Switched Telephone Network

SA Satellite Access
 SAT Subscriber Access Termination
 STE Secure Telephone Equipment
 SUT System Under Test
 SWT Sectéra® Wireline Terminal
 SX-12 Simulator, Data Link
 T1 Digital Transmission Link Level 1 (1.544 Mbps)
 TDM Time Division Multiplexing
 VoIP Voice over Internet Protocol

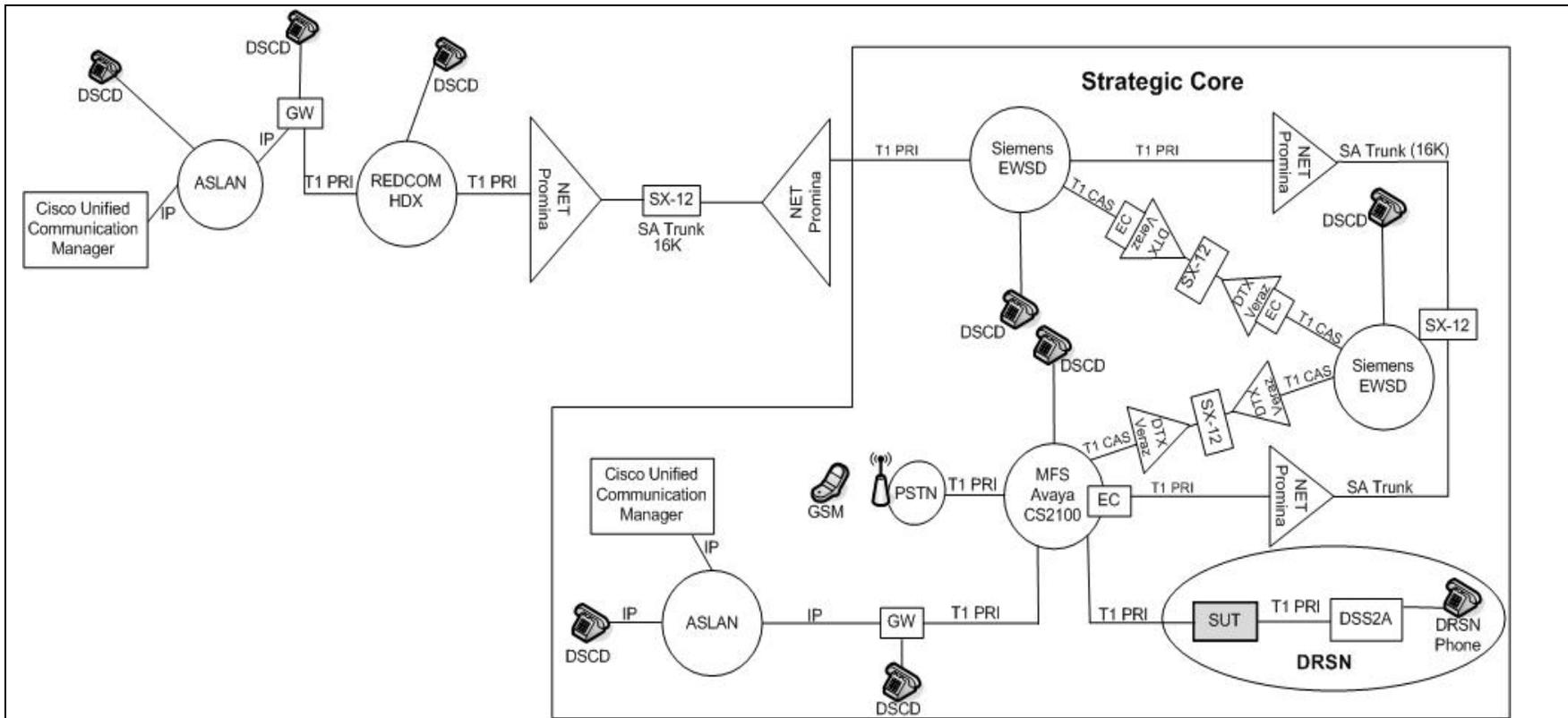
Figure 2-5. CENTCOM Composite Test Diagram



LEGEND:

ASLAN	Assured Services Local Area Network	IP	Internet Protocol	STE	Secure Telephone Equipment
CAS	Channel Associated Signaling	JCSE	Joint Communications Support Element	SUT	System Under Test
CEU	Channel Encryption Unit	K	Kilobit	SWT	Sectéra® Wireline Terminal
CS2100	Communication Server 2100	Mbps	Megabits per second	SX-12	Simulator, Data Link
DSCD	Department of Defense (DoD) Secure Communications Device	MFS	Multifunction Switch	T1	Digital Transmission Link Level 1 (1.544 Mbps)
EC	Echo Canceller	NET	Network Equipment Technology	TDM	Time Division Multiplexing
EWSD	Elektronisches Wählsystem Digital	PRI	Primary Rate Interface	TDMA	Time Division Multiple Access
GSM	Global System for Mobile Communications	PSTN	Public Switched Telephone Network	VoIP	Voice over Internet Protocol
GW	Gateway	SA	Satellite Access	VX	Voice Exchange

Figure 2-6. JCSE DSCD Composite Test Diagram



LEGEND:

ASLAN	Assured Services Local Area Network	GW	Gateway	SA	Satellite Access
BRI	Basic Rate Interface	HDX	High Density Exchange	STE	Secure Telephone Equipment
CAS	Channel Associated Signaling	IP	Internet Protocol	SUT	System Under Test
CEU	Channel Encryption Unit	K	Kilobit	SWT	Sectéra® Wireline Terminal
CS2100	Communication Server 2100	Mbps	Megabits per second	SX-12	Simulator, Data Link
DSCD	Department of Defense (DoD) Secure Communications Device	MFS	Multifunction Switch	T1	Digital Transmission Link Level 1 (1.544 Mbps)
EC	Echo Canceller	NET	Network Equipment Technology	TDM	Time Division Multiplexing
EWSD	Elektronisches Wählsystem Digital	PRI	Primary Rate Interface	VoIP	Voice over Internet Protocol
GSM	Global System for Mobile Communications	PSTN	Public Switched Telephone Network	WIN-T	Warfighter Information Network - Tactical

Figure 2-7. WIN-T Composite Test Diagram

received an Authority To Operate from NSA on 20 January 2012, which meets this requirement.

(2) The UCR 2008, Change 3, paragraph 5.2.2.2, states that DSCD devices that use a 2-wire analog or BRI interface shall meet the EI requirements as specified in Section 5.2.1, Customer Premises Equipment Requirements. The DSCD devices that use an IP interface shall meet the EI requirements as specified in Section 5.3.2, Assured Services Requirements. DSCD devices that support DSN trunk interfaces (PRI or IP (AS-SIP)) shall meet the interface requirements defined in 5.3.2.12.10, MG support for ISDN PRI Trunks, for PRI and 5.3.4 for AS-SIP. The SUT met the capability and functional requirements for an ISDN PRI NI2 interface in accordance with UCR section 5.3.2.12.10 with the following minor exception: The SUT does not support ISDN B Channel Availability (Service Messages). The SUT does acknowledge or have the ability to initiate in-service or out-of-service Service Messages. To mitigate the impact of this discrepancy, the respective B channels must be busied out by both switches at each end of the circuit. DISA adjudicated this as having a minor operational impact based on the stipulation that this condition be noted in the SUT deployment guide. The vendor has no plans to fix this anomaly based on the following: The SUT is typically deployed in a local location resulting in short runs between the device and the high side and low side switches. This has resulted in there not being a customer requirement to automatically set the availability of channels. This requirement was met by both testing and the vendor's LoC.

(3) The UCR 2008, Change 3, paragraph 5.2.2.2, states that a DSCD device that supports one of the required signaling modes shall interoperate with and establish secure session with other compatible devices with at least a 85 percent secure call completion rate. The SUT had a 98 percent completion rate, which meets this requirement.

(4) The UCR 2008, Change 3, paragraph 5.2.2.2, states that the DSCD shall be capable of using the protocols provided to establish a secure session within 60 seconds and must maintain secure communications for the duration of the secure portion of the call. The SUT setup secure calls over the test configurations depicted in Figures 2-2 through 2-8. All calls established a secure connection within 35 seconds and maintained calls until sessions were ended, which meets this requirement.

(5) The UCR 2008, Change 3, paragraph 5.2.2.2, states that the DSCD shall operate in a network that has an end-to-end latency of up to 600 milliseconds (ms). The SUT was able to establish secure calls over the test configurations depicted in Figures 2-2 through 2-9. The maximum end-to-end latency was 800 ms configured for Public Switched Telephone Network analog interface using SCIP signaling, which met this requirement.

(6) The UCR 2008, Change 3, paragraph 5.2.2.2 states the DSCD shall achieve and maintain a secure voice connection with a minimum MOS of 3.0. The SUT

achieved and maintained a secure voice connection with a MOS of 3.7, which meets this requirement.

(7) The UCR 2008, Change 3, paragraph 5.2.2.2, states that a DSCD shall obtain a new key and properly process the new key with a 95 percent completion rate. The SUT does not receive rekey updates via the Key Management Center. Instead, the SUT supports rekey with the use of an AN/CYZ-10 Data Transfer Device which is acquired from local communications security custodian. The SUT was keyed using this process 100 percent of the time with no failure, which meets this requirement.

12. TEST AND ANALYSIS REPORT. No detailed test report was developed in accordance with the Program Manager's request. JITC distributes interoperability information via the JITC Electronic Report Distribution (ERD) system, which uses Unclassified-But-Sensitive Internet Protocol Router Network (NIPRNet) e-mail. More comprehensive interoperability status information is available via the JITC System Tracking Program (STP). The STP is accessible by .mil/gov users on the NIPRNet at <https://stp.fhu.disa.mil>. Test reports, lessons learned, and related testing documents and references are on the JITC Joint Interoperability Tool (JIT) at <http://jit.fhu.disa.mil> (NIPRNet). Information related to DSN testing is on the Telecom Switched Services Interoperability (TSSI) website at <http://jitc.fhu.disa.mil/tssj>. Due to the sensitivity of the information, the Information Assurance Accreditation Package (IAAP) that contains the approved configuration and deployment guide must be requested directly through government civilian or uniformed military personnel from the Unified Capabilities Certification Office (UCCO), e-mail: disa.meade.ns.list.unified-capabilities-certification-office@mail.mil.